Type II codes over $\mathbf{F}_2+u\mathbf{F}_2$ and an application to Hermitian modular forms (Algebraic Combinatorics)

AUTHOR(S):

坂内, 英一; 原田, 昌晃; 宗政, 昭弘; 大浦, 学

数理解析研究所講究録
1109巻 1999年 22-25

Type II Codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and An Application to Hermitian Modular Forms

九州大・数理 坂内 英一 (Eiichi Bannai)
山形大・理 原田 昌晃 (Masaaki Harada)
九州大・数理 宗政 昭弘 (Akihiro Munemasa)
九州大・数理 大浦 学 (Manabu Oura)

本講演では、有限環 $\mathbb{Z}[i]/2\mathbb{Z}[i]$ 上の self-dual code のあるクラスである Type II code についての紹介をし、その分類が binary Type II code の分類から得られることを述べた。また、$\mathbb{Q}[i]$ 上の symmetric Hermitian modular form of genus 2 を、Type II code の symmetrized weight enumerator polynomial に theta constants を代入することによって構成し、知られている Hermitian modular form の6つの生成元のうち weight が4の倍数になっているものがすべてこの方法で得られることを示されることを紹介した。ここに書かれてある結果は、準備中の論文 [1] に書かれる予定であるので、詳しい証明等をそちらをご覧いただきたい。

まず、有限環 $\mathbb{Z}[i]/2\mathbb{Z}[i]$ 上の self-dual code の定義から始める。以後 $R = \mathbb{Z}[i]/2\mathbb{Z}[i] = \{0, 1, i, u\}$, $u = 1+i$ と書き、R^n の R-submodule を長さ n の R-code (または R 上の code) と呼ぶ。R^n 上の内積 $(x, y) = \sum_{j=1}^{n} x_j y_j$ を考え、この内積に関する R-code C の直交補空間を $C^{\perp}$ と書く。C が $C = C^{\perp}$ を満たすとき self-dual であるという。R^n のベクトル x に対して、x の weight を $\mathrm{wt}(x) = |\{j | x_j = 1 \text{ or } i\}| + 2|\{j | x_j = u\}|$ で定義する。Self-dual R-code C がさらに、$\mathrm{wt}(x) \equiv 0 \pmod 4$, $\forall x \in C$ を満たすとき、C は Type II code であるという。二つの R-code C_1 と C_2 が座標の入れ換えおよび適当な座標の成分の 1 と i を入れ換えることによって一致するときに、この二つの code は同値であるという。次に、写像 $\alpha : R \to \mathbb{F}_2^2$ を $\alpha(0) = (0,0)$, $\alpha(1) = (0,1)$, $\alpha(i) = (1,0)$, $\alpha(u) = (1,1)$, によって定義し、これを写像 $\phi : R^n \to \mathbb{F}_2^{2n}$ へ自然に拡張する。この写像 ϕ を Gray map と呼ぶ。

Lemma 1. 二つの R-code C_1 と C_2 が同値であることと $\rho(\phi(C_1)) = \phi(C_2)$ なる元 $\rho \in C_{S_{2n}}(\tau)$ が存在することは同値である、ただし ϕ は Gray map を表し、また $C_{S_{2n}}(\tau)$ は $\tau = (1,2)(3,4)\cdots(2n-1,2n)$ の S_{2n} における中心化群を表す。

集合 $\mathcal{D}$ を、長さ $2n$ の binary code D と、その自己同型群 $\mathrm{Aut}D$ に属する fixed point free involution τ の組 (D,τ) 全体のなす集合とし、$\mathcal{D}$ に次のような同値関係を定義する：$\rho(D_1)=D_2$ かつ $\rho\tau_1\rho^{-1}=\tau_2$ なる元 $\rho\in S_{2n}$ が存在するときに、(D_1,τ_1) と (D_2,τ_2) が同値であると定義する。ここで、(D,τ) を含む同値類を $[D,\tau]$ で表すことにする。また、同値類全体の集合を $\bar{\mathcal{D}}$ とかくことにする。$\mathcal{C}$ を R 上の長さ n の code の集合とし、各 $C\in\mathcal{C}$ に対して、C を含む同値類を $[C]$ で表すことにする。長さ n の R-code の同値類の集合を $\bar{\mathcal{C}}$ とかく。このとき、Lemma 1 によって次の結果が得られる。

Proposition 2. $[C]\mapsto[\phi(C),\tau]$ によって、$\bar{\mathcal{C}}$ と $\bar{\mathcal{D}}$ の間に一対一の対応が与えられる。

R 上の Type II code の Gray map の像は binary Type II code であるので Type II R-code は長さが 4 の倍数でのみ存在することが分かる。さらに Proposition 2 によって、長さ $2n$ の binary Type II code の分類とその自己同型群の fixed point free involution の共役類の分類が、R 上の長さ n の Type II code の分類を与えることが分かる。

長さ 4 と 8 の R 上の Type II code の分類は [3] で行われている。ここでは、長さ 12 の分類を上の方法で行なった。長さ 24 の binary Type II code の分類は [6] で行なわれており、ちょうど 9 個の非同値な code が存在する。これら 9 個の code から上の分類方法により、長さ 12 の R 上の Type II code は 82 個存在することが求められた。講演時には、長さ 16 の分類は完了していなかったが、その後長さ 32 の binary Type II code の分類 [2] (85 個の非同値な code が存在) を用いて、この分類も完成した。

Proposition 3. 長さ 12 の R 上の Type II code は同値を除いてちょうど 82 個存在する。また、長さ 16 の R 上の Type II code は同値を除いてちょうど 1894 個存在する。

注意：binary Type II code の分類は長さ 32 までしか完成していないので、長さ 20 の Type II R-code の分類は上の方法では行なえない。

次に R^2 の部分集合 A を次で定義する。

$$A=\{(0,0),(0,1),(0,u),(1,0),(1,1),(1,i),(1,u),(u,0),(u,1),(u,u)\}$$

R^n の2つのベクトル x, y と $a \in A$ に対して、

$$N_a(x,y) = |\{j|(x_j, y_j) = a \text{ or } ia\}|$$

とおく。A の元で index された 10 個の変数 X_a $(a \in A)$ を用意し、C の symmetrized weight enumerator polynomial を次で定義する。

$$\mathrm{swe}_C(X_a; a \in A) = \sum_{x,y \in C} \prod_{a \in A} X_a^{N_a(x,y)}.$$

すると C の長さが n のとき $\mathrm{swe}_C(X_a; a \in A)$ は n 次 homogeneous polynomial になる。さらに C が Type II code のときは、$\mathrm{swe}_C(X_a; a \in A)$ はさまざまな不変性をもち、位数 737280 の $GL(10, \mathbb{Q}[i])$ のある部分群の作用によって不変であることがわかる。この不変性と theta constants

$$f_a(\tau) = \sum_{x \in \mathbb{Z}[i]^2} \exp 2\pi i((x + \frac{1}{2}a)^* \tau (x + \frac{1}{2}a))$$

の間の変換公式から、$\mathrm{swe}_C(f_a(\tau); a \in A)$ は $\mathbb{Q}[i]$ 上の symmetric Hermitian modular form of weight n になることがわかる。すなわち、ある 10 次有限行列群の不変式環から、$\mathbb{Q}[i]$ 上の symmetric Hermitian modular form のなす環への準同型写像ができたことになる。

さて、$\mathbb{Q}[i]$ 上の symmetric Hermitian modular forms の作る環の生成元は Freitag [4], Nagaoka [5] により与えられている。Nagaoka [5] によれば、

$$\mathbb{C}[\psi_4, \psi_8, \psi_{12}, \psi_{16}, \chi_{10}, \chi_{16}]$$

が $\mathbb{Q}[i]$ 上の symmetric Hermitian modular forms の作る環と一致する。ここで subscripts はすべて weight を表している。($\psi_4, \psi_8, \psi_{12}, \psi_{16}, \chi_{10}, \chi_{16}$ の定義は [5] を参照)。

自然数 n に対して、成分がすべて 1 である R^n のベクトルを $\mathbf{1}_n$ で表し、$R\mathbf{1}_n$ の直交補空間を P_n と書き、$K_n = R\mathbf{1}_n + uP_n$ とおく。n が 4 の倍数のときは K_n は Type II code になり、

$$\mathrm{swe}_{K_n}(f_a(\tau); a \in A) = \psi_n \quad n = 4, 8, 12, 16$$

となることが両辺の Fourier 係数を比較することによって得られる。χ_{12} 自身は $\mathrm{swe}_C(f_a(\tau); a \in A)$ という形に表すことはできないが、上で求めた長さ 12 の Type II R-code の分類を用い、それらに対応する Hermitian modular form をすべて求めることにより、以下の結果が得られた。

Theorem 4. Symmetric Hermitian modular forms $\mathrm{swe}_C(f_a : a \in A)$ (ただし C は Type II R-code 全体を動く) で生成された環は、$\psi_4, \psi_8, \psi_{12}, \psi_{16}, \chi_{12}$ を含む。

参考文献

[1] E. Bannai, M. Harada, A. Munemasa and M. Oura, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and applications to Hermitian modular forms, (in preparation).

[2] J.H. Conway, V. Pless and N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *J. Combin. Theory Ser. A* **60** (1992), 183–195.

[3] S.T. Dougherty, P. Gaborit, M. Harada and P. Solé, Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inform. Theory* **45** (1999), 32–45.

[4] E. Freitag, Modulformen zweiten Grades zum rationalen und Gaußschen Zalhkörper, Sitzungsber. Herdelb. Akad. Wiss., (1967).

[5] S. Nagaoka, A note on the structure of the ring of symmetric Hermitian modular forms of degree 2 over the Gaussian field, *J. Math. Soc. Japan* **48** (1996), 525–549.

[6] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A* **18** (1975), 313–335.